Identity fraud as a challenge to the constitutional state[1]

By Dr *mr* J.H.A.M. Grijpink[2]

Summary

This article explains that not only the arsenal of identity instruments, but also our identity verification methods have to change if we are to meet the challenge of identity fraud in the future. Existing identity policies are not up to the task of guaranteeing our security and privacy in an information society. Because of the prevailing legal-administrative approach, more vigorous procedures and new technologies often backfire. Therefore, this article calls for a new approach to identity verification that effectively frustrates and combats identity fraud. It presents an analysis based on Dutch law, but the conclusions will be valid in most western constitutional states. Some suggestions are presented to improve the quality of identity checks. Dutch law appears to offer sufficient starting points to achieve this.

1. Introduction

Since the events of 11 September 2001, identity issues have been high up on the agenda of many Western countries. All over the world, in countries with highly different legal cultures, a great deal of effort is being spent improving the identity management and tightening up the policy governing identity verification in order to enhance security. Countries without or with only limited compulsory identification such as the Netherlands are now considering the introduction of general compulsory identification. Countries without laws for general compulsory proof of identity, such as the United Kingdom, are now taking steps to introduce this identity instrument. Moreover, many countries are giving consideration to adding a biometric feature[3] of the holder to identity cards and travel documents. Only biometric identity verification uses body-related characteristics to make sure that a document or object belongs to the person using it. All other verification procedures are based on administrative details without a direct link with the person involved.

The purpose of a more stringent identity policy is to enable the establishment of someone's identity or the verification that the person involved is the right one in increasingly more situations and with greater reliability. The importance of the distinction between these two forms of identity check is that verifying that someone is the right person doesn't necessarily require knowledge of who he is. Even if the events of 11 September 2001 had not taken place, this aim would still have gained more importance in keeping with the growing number of transactions that are conducted electronically and at a distance without social control or visual supervision. Electronic communication spans the whole world and in the coming years gains extra dimensions through the increasing mobility and anonymity of society. Identity checks, too, are more and more likely to be performed electronically and at a distance. This is why we will need a broad arsenal of identity instruments for person recognition and identity verification in the future. In addition to what we already have, such as electronically readable identity cards, pass numbers, personal numbers, pin codes and passwords, this will also have to include functions such as electronic signatures and biometrics.

[1] This article is based on a series of previous publications, in particular *Informatiestrategie voor ketensamenwerking* ('Information strategy for chain co-operation), Sdu Uitgevers, The Hague, 2002, ISBN 90 1209 697 9, *Biometrics and Privacy*, in: Computer Law and Security Report, May/June 2001, vol. 17 (3) 2001, pp. 154-160, Elsevier Science Ltd, Oxford, UK , ISSN 02673649 and *Personal numbers and identity fraud, number strategies for security and privacy in an information society*, in: Computer Law and Security Report, vol. 18 (5) 2002, pp. 327-332 (Part I) and vol. 18 (6) 2002, pp. 387-395 (Part II), Elsevier Science Ltd, Oxford, UK, ISSN 02673649

[2] Dr mr J.H.A.M. Grijpink, economist and lawyer by education and information strategist by profession, is Principle Advisor at the Strategy Development Department of the Netherlands Ministry of Justice. In 1975 he obtained a postgraduate degree in management consultancy at the Stichting interacademiale opleiding organisatiekunde (SIOO) and in 1997 his Ph.D. at the Technical University of Eindhoven. He is a Certified Management Consultant (CMC) and a Registered Information Expert (RI).

[3] This is a body-related characteristic, for instance the fingerprint or the voice, that can be used as a digital key to get or give access to processes and data or to recognise somebody by electronic means.

2. Identity fraud

In the western world the identity policy concentrates mainly on combating document fraud, namely the use of counterfeited legal identity documents. The fraudulent use of a valid identity document officially belonging to someone who closely resembles the user (so called lookalike fraud) is already compelling us to face up to the problem of identity fraud. This means that somebody with dishonest intentions deliberately passes himself off under an identity that does not belong to him by using the identity of another existing or fictitious person. Identity fraud doesn't necessarily require the use of an identity document. The identity fraudster can make use of personal numbers, photos, actions or occurrences as well, because they all feature an identity suggestion from which people draw conclusions about whom they are dealing with. Therefore, identity fraud can take place anywhere and in many ways and is not restricted to specific situations, procedures or documents. Once a person has fraudulently changed his identity, the new 'identity' can affect other situations along regular channels. In these situations it usually is no longer possible to see through the preceding fraudulent identity change. Identity fraud is often the first step towards a subsequent fraud, such as a bank fraud, a passport fraud or a benefit fraud. But these application-based fraud specifications distract our attention from the common denominator of these forms of fraud, which is that a cunning method is used to deliberately misuse the identity of an existing or fictitious person. When it comes to combating identity fraud, combating counterfeited identity documents is no longer where the normative focus should be placed. The main focus should not be the identity document but the person using it. In the same way, the quality of the identity document is no longer the dominant factor, but the quality of the verification process itself in the given situation.

3. Identity fraud calls for a different identity policy

Identity fraud is forcing us to take a fresh look at the parameters, function and use of identity instruments in our legal culture. It often turns out that measures and instruments that are useful in combating document fraud do not provide solutions to identity fraud. Often they have the reverse effect. Thus, the way in which we use information technology for identity verifications is also placed in a different light.

Three examples to illustrate this:

a. *Giving the social security number in the Dutch passport elicits fraud*
This is an identity measure that dates back to 1996 and was intended to make it possible to use identity documents for name-number verifications so that it becomes easier to establish someone's social security number. This name-number verification is effective if the identity document is sound and the holder is the right person. But that is no longer the case if someone else who closely resembles the rightful holder uses the identity document. After all, a name-number verification based on an identity document always succeeds, regardless of who is making use of the document. A person who holds an identity document belonging to someone else, for example, can assume that identity without being noticed and thus have a free ride with that person's social security number. Furthermore, there are many verification situations in which it is practically sufficient to hand over a copy of an identity document. This copy can easily be adapted for use by somebody else. Giving the social security number in identity documents (e.g. the Dutch passport and driving licence) therefore inadvertently makes identity fraud much easier.

b. *The identity document increases the predictability of the verification*
Identity documents and identity checking procedures are governed by regulations. These regulations unintentionally play into the hands of the identity fraudster. They enable him to predict where, when, how and by whom his identity will be checked. Moreover, identity verification procedures are often public and can be inconspicuously observed in order to establish weak points in the technology, the organisation or the procedures. With a certain amount of preparation, an identity fraudster can outwit most identity checks.

c. *Legal standards hinder the approach to identity fraud*

Identity fraud also places some underlying legal standards in a different light. To give an example, the legal standard that a person is innocent until proved guilty. This corresponds with a general standard in our legal culture that there must be reasonable grounds for suspicion. That means that we may not and cannot be constantly alert to identity fraud. We have to put on hold our need to check someone's identity until there is a serious suspicion that someone is acting in bad faith. By that time, it is usually too late. The identity fraudster can no longer be found or has to be left alone because of a lack of evidence. Not even the government is permitted without legal provisions to avail itself of compulsory procedures that check everybody on the basis of a general suspicion. Without such a legal provision, this would only be lawful if that check was made on a voluntary basis, which means that the person in question must be informed in advance. The element of surprise is thus only enjoyed by the identity fraudster.

These examples underline the fact that all existing identity measures and instruments must be tested for their effectiveness in combating identity fraud. We are thus given a clear picture of the challenge of identity fraud in a constitutional state. This gives us a different perspective on the way in which we verify identities and use (information) technology for this purpose. But that is not where it ends. The law, too, appears to be facing a challenge in adapting to the new requirements of an increasingly complex information society.

4. The legal framework of the current Dutch identity policy

In Dutch private law, there are generally no sanctions for not giving your identifying personal details or using another, possibly fictitious, identity. And quite right, too. After all, how would people otherwise be able to remain anonymous for good reasons such as personal security on the Internet? There is no reason to infringe on the freedom of contracting parties to come to an agreement using a pseudonym or even remaining anonymous. A public authority that needs to know a person’s identity to adequately accomplish its public task is entitled to ask for someone’s identifying personal details. This person has the right to keep silent, even in criminal procedures, but giving false personal details to a competent public authority is regarded as a (minor![4]) public order offence (Netherlands Penal Code, article 435). Keystones of this general legal framework are the Dutch Data Protection Act and the Access to Public Documents Act. The former prescribes from a privacy protection viewpoint when authorities are permitted to retrieve, use or store personal details. The latter regulates public access to relevant government information and documents.

In addition to these general laws, the Dutch identity policy is also based on specific laws and regulations. These include the Compulsory Identification Act (1993) for a limited number of situations in which people have to identify themselves, the Local Residents’ Registration Act for the administration of identifying personal details of residents and some special laws providing for legal proof of identity, such as the Passports Act. And then there are laws that provide for the issue and use of official personal numbers, such as the General Law on State Taxes for the social security number. This legal framework clearly specifies when identity checks must be carried out, indicates the verifying authorities and, usually, even the procedure to be followed and which identity documents should be used. It provides a few official identity documents with a monopoly position when it comes to identity checking. In our legal culture, this results in identity verifications being highly predictable, uniform and observable, while the element of surprise is only the identity fraudster’s. Predictability, uniformity and publicity do not get in the way of combating counterfeit identity documents, but form less suitable starting points for combating identity fraud.

[4] This relatively light classification with ditto punishment doesn’t really put up barriers for someone who thus wants to make himself untraceable. The lawmaker clearly considers this offence as a stand-alone misdemeanour and not as the preparatory phase and success factor for all sorts of crimes, even capital crime.

Fortunately, the current law appears also to offer starting points to the verifying authority for more elements of surprise and variation, but at present these are barely being used. This will be the case when a public body that is authorised by law to give specific instructions to other verifying agencies, succeeds in keeping these verification instructions undisclosed. For the purpose of identity verification this will not be against the law, because according to article 10 paragraph 2 of the Access to Public Documents Act, these external instructions do not have to be disclosed if one of the exemption criteria is applicable. This refers in particular to the exemption criteria 'the investigation and prosecution of criminal offences' and 'inspection, verification and supervision by administrative bodies'. Legal precedence from the Supreme Court of the Netherlands shows that for the first criterion a specific suspicion is not required, which means that general instructions for more varied identity checks that are less predictable for the person being checked, can also come under this criterion.

5. The legal-administrative character of the current identity policy

Identity fraud can be regarded as a phenomenon that makes identity management and identity verifications more complex and – in response to this – elicits administrative measures to regain control of the increased complexity. Identity documents, personal numbers and biometrics, each with the appropriate operating procedures, are relevant administrative instruments in this context. As new developments occur these are further improved, for instance, by adding new security techniques to identity documents or new information and by applying new technology to identity verification procedures. The aim of these measures is to reduce the increased complexity in the first place. This legal-administrative approach is characterised by the pursuit of simplicity, uniformity and transparency. Viewed from the perspective of the requirements of public administration, there is nothing wrong with that. On the contrary, order benefits from known and clear information, uniform instruments and predictable methods. On the other hand, this approach has made our identity verification procedures step by step more transparent, uniform and predictable to the benefit of the identity fraudster. This approach is in stark contrast with what living organisms in nature do if the environment becomes more complex. They do not opt to reduce complexity, on the contrary. They adapt themselves to the increased complexity of their environment by making themselves more complex, through increasing internal differentiation, by more behavioural variation and, especially, by putting in place extra feedback mechanisms. Obviously, in nature it seems that better observation of the environment forms a better starting point for regaining control of the increased environmental complexity. Simplified or uniformed instruments and predictable or transparent procedures of identity verification, however, yield the contrary, most of all fewer observation possibilities and feedback mechanisms.

Three examples illustrating this analysis are:

a. *The biometric passport*

   To combat a specific type of identity fraud – the use of a passport by somebody who resembles the rightful owner (lookalike fraud) – a draft bill was recently introduced to the Dutch Lower House with the intention of amending the Passport Act so that a biometric template[5] can be shown on the new Dutch passport, in the same way as the social security number has been given in identity documents since 1996. The advantage of this is that biometric identity checks become possible in situations subject to compulsory identification because the passport is our most important legal identity document. This is going to make passport biometrics the de facto general standard for biometric identity verification in the Netherlands, in the same way as the social security number shown in identity documents is gradually becoming the Dutch general

[5] A biometric template is a number that is calculated using typical features of a body-related characteristic, e.g. the location in a fingerprint where lines join or separate or show interruptions. This number is recalculated at the moment of identity check. If the new value corresponds more or less with the reference value, the person checked is supposed to be the same person as the person that was measured in the first place.

personal number[6]. The downside of this approach to put the social security number or the biometric template *on* identity documents that show the holder's identifying personal details is, that it makes things easy for the identity fraudster. He knows beforehand that any name-number verification will be successful even if he uses somebody else's identity document. In future the identity fraudster will also know the measurement value that his biometric reading has to meet. Often, this can be taken care of. The current biometric devices are easy to mislead and the current biometric techniques cannot be organised as to resist fraud if used on a wide scale. With patient observation the identity fraudster can discover weak spots in an identity checking process and come up with a method that guarantees his success. New technology thus unintentionally yields the opposite of what is expected of it: instead of better identity verification, more identity fraud!

b. The citizen service number (CSN)

The second example is a recent proposal of the Dutch government to introduce a compulsory public general personal number, known as the Citizen Service Number (CSN). Personal numbers have gradually begun to take on an important role, both for the administrative linking and protection of personal details and for identifying people[7]. As a result of this, the misuse of personal numbers has become an increasingly significant form of identity fraud. Viewed from the perspective of the traditional legal-administrative approach, an obvious countermeasure is to introduce a general public personal number that

– people are compelled to use in a wide range of situations, irrespective of the supported processes and regardless of the problem that the number is intended to resolve in a specific situation (this reflects the legal-administrative pursuit of simplicity, uniformity and predictability)

– should be stated *on* all legal identity documents (this reflects the legal-administrative pursuit of uniformity, publicity and cognizability).

In fact, combating identity fraud will in the future require a more differentiated personal number policy using a lot of independently managed sector numbers that can be mutually compared if necessary and with appropriate procedures. General personal numbers may be indispensable to cross-link sectoral numbers thus bringing identity fraud to light. Therefore, the general personal number should not adversely affect or oust sectoral personal numbers. This implicates that the general personal number should not be compulsory and public, nor be distributed or used for external communication. The use of many sectoral personal numbers makes identity fraud more apparent and yields more verification options and feedback mechanisms compared with the use of a single all-purpose compulsory number. A sectoral approach diminishes the vulnerability of personal number systems to data contamination, system malfunctioning, errors and fraud. Taken on its own, any sectoral number is less valuable and attractive to the identity fraudster than the general number would be. Moreover, it becomes more difficult to predict – in comparison with a situation with only one general personal number – when, where and how he will come up against problems because he cannot foresee which other personal numbers he has to keep consistent with each other in order to avoid standing out.

On the other hand, the compulsory general use of a single general public personal number inevitably makes its value disproportionately great, so that this personal number system becomes vulnerable to improper use, errors and fraud. At the same time, verification alternatives decrease because the compulsory use of the general public number will mean that fewer independent sector numbers will be maintained. This is a serious disadvantage, because the management of a general personal number

[6] A general personal number is a unique number allocated to somebody to be generally used for the purpose of registration and administrative linking of personal details of the same person. Other personal numbers are not for general purpose, but are linked, for instance, to an information system (e.g. a telephone number), an organisation (client number) or to a process (the drug addiction number used in the treatment and care of drug addicts).

[7] *Personal numbers and identity fraud, number strategies for security and privacy in an information society,* in: Computer Law and Security Report, vol. 18 (5) 2002, pp. 327-332 (Part I) and vol. 18 (6) 2002, pp. 387-395 (Part II), Elsevier Science Ltd, Oxford, UK, ISSN 02673649

system is usually inadequate. This number management should in fact be at the quality level required by the most demanding sector, but in other sectors there is often a lack of support for the extra costs, so that people make do with a minimum effort. Thus, opting for a general public and compulsory personal number might seem less complicated and therefore more attractive, but such an approach offers less opportunities for combating identity fraud and for protecting people's privacy in an information society.

c. *Compulsory identification in hospitals*

The third example is the introduction of compulsory identity verification in the Dutch health care. 'On 17 April 2003 the cabinet approved the proposal of Minister of Health, Welfare and Sports (VWS) de Geus to introduce legal compulsory identification in hospitals and outpatients', with the later addition of district nursing, psychiatry, care and nursing homes and care for the handicapped. Patients now identify themselves with a health pass issued by the health insurer. This has also become the subject of fraud on a wide scale.'[8] The intention of the minister is to use this measure to combat fraud in the healthcare sector. Hospitals and outpatients' clinics that fail to verify the identity of their patients are no longer able to claim their expenses from the National Health Service.

This example, again, illustrates an underestimation of the fraud problem. In most cases, it is not a matter of counterfeited health passes, but of identity fraud. You may wonder if the best approach is a closer scrutiny of the health care pass using an official identity document. The health care workers have no expertise to deal with identity checking. The remedy might be worse than the disease if the compulsory identification with the social security number on a silver platter, in the long run will cause the social security number to be broadly used as access to the (electronic) medical file[9]. This strongly contaminated and poorly managed personal number will cause irreparable chaos in the health care sector, resulting in many medical errors and undertreatment.

It is worthwhile to take a slightly closer look at our traditional legal-administrative approach. This approach features a number of principles that hinder us when it comes to combating identity fraud. They sometimes even prevent us from noticing identity fraud.

a. Every identity instrument (identity card, personal number, PIN, biometrics) provides *identity suggestions*, which causes people to assume they know whom they are dealing with. While checking someone's identity we tend to look at the identity instrument as such and to overlook these identity suggestions. That is why identity fraud usually succeeds, by way of simply accepted identity suggestions that can no longer be seen through during later identity checks elsewhere.

   To give an example, the Dutch government regards the Dutch social security number as being purely an administrative number from which no rights can be derived, although the number implies the identity of its legal owner even if somebody else is using it. With someone else's social security number an illegal immigrant can be included on the payroll of an employer or receive social security benefits in someone else's name. This identity fraud cannot be prevented by a number-name check on the basis of an identity document of the legal owner of this social security number. After all, this number-name check always succeeds because the social security number mentioned on an identity document truly belongs to the legal holder of the document.

b. We spontaneously tend to trust administrative identities, even though they are often based on unverified or unverifiable personal details. While issuing an identity document or personal number, be it inside or outside of the government, we unknowingly derive incorrect details from source documents, because we are not able to verify the integrity or authenticity of the document and the true relation to the person presenting it. In many cases, an information infrastructure designed to frustrate identity

[8] Quoted from NRC of Friday 18 April 2003

[9] See J.H.A.M. Grijpink, *Informatiestrategie voor ketensamenwerking* [Information strategy for chain co-operation], Sdu, Uitgevers, The Hague, 2002, pp. 65 ff and especially p. 77

fraud by blocking an identity document or a personal number against use by others against the will of the rightful holder does not exist or may not be used.

c. When checking someone's identity we spontaneously ask the question 'who are you', whereas it is usually sufficient to know for sure that someone is the right person, regardless of whom he is. Using a biometric characteristic, for example, somebody can be accurately identified as the right person even if we cannot find out who he is. Carefully and independently managed private and public pseudonyms (personal numbers, pin codes, passwords, electronic signatures, etc.) facilitate all sorts of accurate identity verifications, which can thus be made more varied and less predictable. This is a way of effectively combating the tendency to ritualise identity checks. We often leave these opportunities unused by this unnecessary emphasis on *'identity'* that causes us to forget that *anonymous* and *semi-anonymous* identity checks are also possible[10].

These starting points, which are inadequate for combating identity fraud, are mutually reinforcing. They explain why, despite all our good intentions, we spontaneously take identity measures that unintentionally increase rather than reduce the opportunities to commit identity fraud. The most important consequence of the approach to the 11 September problem will therefore probably be that tightening up the prevailing identity policy will play into the hands of the identity fraudster and that, despite all our good intentions, identity fraud will increase in scope and seriousness.

6. New solutions for the Dutch identity policy

In the Dutch identity policy identity fraud should be the reference point for new solutions getting at better identity checking procedures. We conclude that the current legal framework has given a monopoly position to a number of legal identity documents and has made identity checks extremely predictable for the identity fraudster. These conclusions should lead to a critical review of what we are actually checking in a standardised identity check based on a legal identity document only. Can this amount to more than ascertaining the authenticity of the identity document? If we only have the personal details given in the identity document at our disposal, how can we actually discover that somebody isn’t the legitimate holder of that identity document? It is precisely those personal details that have enabled the identity fraudster to come up with a plausible story in the first place. Generally, the Dutch Data Protection Act doesn’t permit the verifying authority to simply compare the identity document being presented with other personal details. This may, however, be legal if a structural arrangement for that purpose is made in advance in accordance with the Data Protection Act. But that extra check then simply becomes part of the predictable ritual! This would be so, unless this predictability is offset by targeted identity checking instructions that are kept secret according to article 10 paragraph 2 of the Dutch Access to Public Documents Act. For the time being, we therefore have to conclude that identity fraud falls largely within the ‘blind spot’ of the ritual of our identity verification process.

Combating identity fraud means a different way of thinking and also requires a turnaround in our approach to identity checking. These can be characterised as follows:

– Our attention should shift *from the identity document towards the person using it*. The quality of the document is not unimportant, but not the main issue in combating identity fraud. A persons’ identity can also be checked by other personal details than those mentioned on the identity document. For checking someone’s identity personal details can come from anywhere as long as they aren’t predictable or known to third parties with evil intent. This can legitimately and efficiently be done in an automated way following the approach, which I have described in my publications about value chain computerisation[11]. In any case, the personal details given on the identity document are therefore not suitable at all for identity checking.

[10] Jan Grijpink and Corien Prins, *New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity*, 2001 (2) The Journal of Information, Law and Technology (JILT). Published: 2 July 2001. http://elj.warwick.ac.uk/jilt/01-2/grijpink.html

[11] J.H.A.M. Grijpink, *Chain-computerisation for interorganisational policy implementation* and

- Our attention should shift *from the identity document towards the process of identity checking*. Every situation of identity checking is different, depending on the context of the checking process[12]. In each situation, a successful identity fraud has a different social and economic value, identity checking requires different personal details and chances to prevent identity fraud differ enormously. Thus, identity-checking procedures are to be tailor-made. Predictable standard procedures undermine the effectiveness of any identity checking process.

The problem analysis given above also renders visible the route to other, better solutions. The biggest leverage affect can be expected from elements of surprise built into a varied system of private and public identity verifications, the mutual cohesion of which must be increased without compromising privacy. Effectively combating identity fraud in the near future requires identity-checking procedures to meet a number of extra conditions:

- the predictability of identity verifications should be drastically reduced, for example by various verification procedures with alternating components which, moreover, time and again use different personal details derived from a number of independent sources;
- the monopoly position should be taken away from the legal identity documents, for example, by in various ways involving all sorts of other public and private identity instruments (personal numbers, biometrics, electronic signature) in verification procedures, possibly in combination with the checking partly done from a distance;
- identity checks should be performed, for example, by different verification authorities at different situations and times each using their own variety of procedures and instruments;
- the unique document number should be used more often, because in many cases this number renders the use of a personal number unnecessary;
- no personal numbers should be mentioned *on* an identity document; these personal numbers can well be used as checking details in the background, preferably derived from independent sources elsewhere;
- with confidential checking instructions identity checking procedures should be made more varied and less predictable for the identity fraudster.

In the future, identity fraudsters must no longer be able to find out in advance where, when and how they will run into trouble.

7. Looking ahead

These new conditions mean that the legal framework of the identity policy must be recalibrated. For as long as a public general personal number is given on legal identity documents that occupy a monopoly position for compulsory identity verifications according to the law, the new approach outlined here, aimed at variety and unpredictability, will only gain ground with difficulty. This obstacle should be removed. The legal framework of the Dutch identity policy further seems to offer good starting points for the new approach. Nevertheless, if underlying legal standards still put up barriers, we will also have to adapt ourselves at that level. That is the price that we have to pay to retain our rule of law in an internationalising constitutional state.

Setting out concrete measures for an identity strategy of this nature goes beyond the scope of this article. But what can be said is that some measures that were taken recently by the Dutch government or are due to be taken, anyhow need to be reconsidered because they will probably have the opposite to the desired effect and are also at odds with the new strategy for identity verification to frustrate and combat identity fraud as described above. In the case of the Netherlands, this relates, for example, to

a. the current practice of stating the social security number in legal identity documents;

J.H.A.M. Grijpink, *Chain-computerisation for better privacy protection*, both articles published in: Information Infrastructures & Policy 6 (1997-1999), IOS Press, Amsterdam, maart 2000

[12] In this regard it is important to make a clear distinction from the viewpoint of identity fraud between the different social value chains showing a great variety of fields of forces, opportunities and risks

b. the intended introduction of a compulsory general standardised government application of biometrics using an unchangeable biometric template (especially the fingerprint template) with its intended inclusion *in* the passport;
c. the intended uniform general government application for the electronic signature (what is known as the PKI, the public key infrastructure);
d. the introduction of a compulsory public general personal number, the ‘citizen service number’ (CSN) and its intended mention on identity documents;
e. the introduction of compulsory identification in the healthcare sector.

And finally, the approach to identity fraud called for here implies that general compulsory identification is only an attractive option if it also leads to a more open and varied system of less predictable public and private identity verifications. Unfortunately, the current identity policy cannot be expected to adequately safeguard our security and privacy in the future.